JOURNAL OF NUMBER THEORY 10, 273–290 (1978)

On the First Factor of the Class Number of Prime Cyclotomic Fields

JOHN MYRON MASLEY*

Department of Mathematics, University of Illinois at Chicago Circle, Box 4348, Chicago, Illinois 60680

Communicated by S. Chowla

Received October 3, 1977

Let $H(l)$ be the first factor of the class number of the field $\mathbb{Q}(\exp 2\pi i/l)$, l a prime. The best-known upper and lower bounds on $H(l)$ are improved for small l. The methods would also improve the best-known bounds for large l. It is shown that $H(l)$ is the absolute value of the determinant of an easily written down matrix whose only entries are 0 and 1. The upper bounds obtained on $H(l)$ significantly improve the Hadamard bound on the determinant of this matrix. Results of Lehmer on the factors of $H(l)$ are explained via class field theory.

Let $l = 2d + 1$ be an odd prime number and let $H(l)$ denote the first factor of the class number of the cyclotomic field $\mathbf{Q}(\exp 2\pi i/l)$. Then $H(l)$ is the quotient of the class number of $\mathbf{Q}(\exp 2\pi i/l)$ by the class number of $\mathbf{Q}(\cos 2\pi/l)$.

There are many closed formulas for $H(l)$, but so far exact values of $H(l)$ have been published only for $l \leqslant 257$ (see [5, 15] and also [18]). In this work, we indicate an easy way to extend these tables and also prove some results on the prime factors of $H(l)$. Computations were carried out for all $l < 521$ and will appear elsewhere [10].

In the first section we use the analytic class number formula to derive a simple algebraic expression for $H(l)$. We show that $H(l)$ is the absolute value of the determinant of a matrix whose entries are zeros or ones.

The second section uses analytic methods to derive upper and lower bounds for $H(l)$. The upper bounds facilitate computation of the determinant of Section 1.

The third section is arithmetic in nature. We use class field theory to show that factors of $H(l)$ must lie in certain arithmetic progressions.

* Partially supported by a grant from the National Science Foundation.

0022-314X/78/0103–0273$02.00/0

1. Algebraic Results

In this section we derive an expression for $H(l)$ as the absolute value of the determinant of a 0, 1-matrix. We also give an easy algorithm for writing down this 0, 1-matrix.

Our starting point is the well-known closed formula for $H(l)$ (cf. [5, p. 12] or [6, p. 90]),

$$H(l) = 2l \prod \left(\frac{-1}{2l} \sum_{a=1}^{l-1} \tilde{\chi}(a)\, a \right) \tag{1.a}$$

where the product runs over all odd Dirichlet characters $\tilde{\chi}$ with conductor l. To obtain $H(l)$ as a determinant we will use the following:

Lemma 1.1. *Let G be a finite Abelian group and $\Psi = \mathrm{Hom}(G, \mathbf{C}^*)$ the group of characters of G. Let $f: G \to \mathbf{C}$ be any complex-valued function on G. Then the determinant of the matrix $A = (f(\sigma\tau^{-1}))_{\sigma,\tau}$, where σ and τ run through all the elements of the group G in some fixed order, is given by*

$$\det A = \prod_{\psi \in \Psi} \left(\sum_{\sigma \in G} f(\sigma)\ \psi(\sigma) \right).$$

Proof. See [2, p. 421, problems 12–14].

In order to apply the lemma to the closed formula (1.a) we must make some changes. There are $(l-1)/2 = d$ odd Dirichlet characters mod l. If we choose any one of them, χ say, and fix it, then any odd Dirichlet character $\tilde{\chi}$ mod l is $\tilde{\chi} = \chi\psi$ where ψ is an even Dirichlet character mod l. Our fixed χ then gives a one-to-one correspondence between the set of odd Dirichlet characters mod l and the set Ψ of even Dirichlet characters mod l. We may identify Ψ with the characters of the group

$$G = \mathrm{coker}(\{1 + l\mathbf{Z}, -1 + l\mathbf{Z}\} \to \mathbf{Z}/l\mathbf{Z}).$$

With $\tilde{\chi} = \chi\psi$, $\psi \in \Psi$, as above it is easy to see that $\sum_{a=1}^{l-1} \tilde{\chi}(a)a = \sum_{a=1}^{d} (2a - l)\, \chi(a)\, \psi(a)$. Therefore, we define a function on $\mathbf{Z}$ by putting $f(a) = \chi(a)(a/l - [a/l] - 0.5)$ for an integer a. Since $f(a) = f(a + l)$ and $f(a) = f(-a)$, f may actually be viewed as a function on G.

Via Lemma 1.1 on group determinants we get that $(2l)^{-1} H(l) =$ the absolute value of the determinant of $(f(rc'))_{r,c=1,2,\ldots,d}$ where $cc' \equiv \pm 1 \bmod l$ and $f(rc')$ is the entry in the rth row and cth column. We assume now that c' is the unique integer $1 \leqslant c' \leqslant d$ associated to c such that $cc' \equiv \pm 1 \bmod l$. Since $\chi(rc') = \chi(r)\, \chi(c')$ we may factor $\chi(r)$ from row r, $\chi(c')$ from column c where $r, c = 1, 2, \ldots, d$. The factor pulled out from the determinant is $\prod_{c=1}^{d} \chi(cc') = \pm 1$ and so $(2l)^{-1} H(l) =$ absolute value of the determinant $((2\,\overline{rc'} - l)/2l)_{r,c=1,2,\ldots,d}$ where $\bar{a}$ is the least positive residue of a modulo l.

Note that $\bar{a}/l = a/l - [a/l]$ for positive integers a. We are now in a position to prove.

THEOREM 1.2. *Let l be a prime greater than* 5. *Let $H = (h(r, c))_{r,c=3,4,\ldots,(l-1)/2}$ be the matrix whose (r, c)th entry is $[rc/l] - [(r-1)c/l]$. Then H is a* 0, 1-*matrix and* $|\det H| = H(l)$, *the first factor of the class number of* $\mathbf{Q}(\exp 2\pi i/l)$.

Proof. We will write $m(r, c) = (2l)^{-1}(2\overline{rc'} - l)$ and put $M =$ the $d \times d$ matrix whose rth row and cth column has $m(r, c)$. We have $(2l)^{-1} H(l) = |\det M|$. Multiply the entries in the first column of M by $2l$ and one gets a new matrix N with $H(l) = |\det N|$, $n(r, c) = m(r, c)$ for $c > 1$ and $n(r, 1) = 2r - l$. In particular, $n(d, 1) = -1$ so we may use this entry to zero the other entries of the first column. Now we may ignore the first column and the last row of the resulting matrix which we still denote N. For $c > 1$ we have $n(d-1, c) = [dc'/l] - [(d-1)c'/l] - c'/l - 2n(d, c)$. We can put rows $1, 2, \ldots, d-2$ in this form also by subtracting row $r+1$ from row r for $r = 1, 2, \ldots, d-2$. Now subtract row 1 from each of the rows corresponding to $r = 2, \ldots, d-1$. The entries in these $d-2$ rows now become $[(r+1)c'/l] - [rc'/l]$. In column $c = d$ we have $c' = 2$ so the only nonzero entry in that column (up to row $d-1$) is $-1 = -2/l - 2((2(l-1) - l)/2l)$ in row 1. The theorem follows easily now by rearranging the columns and indexing them by the values of c'.

This theorem was originally proved by Carlitz and Olson [3]. Although the matrix H has easily determined entries, there is a method by which we can write down H with very few divisions.

THEOREM 1.3. *The matrix $H = ([rc/l] - [(r-1)c/l])_{r,c=3,\ldots,d}$ can be written down by putting in* 1's *according to the following scheme and then making every other entry* 0.

(A) *Set a counter $CT = d$ and a "wave number" $WN = 1$.*

(B) *Put $N = (WN)l$. Begin in column $c = 2(WN) + 1$.*

(C) *Divide to find $r = [N/c] + 1$. Put* 1 *in the (r, c)th entry. Put* 1's *in row c from column r through CT inclusive. Set $CT = r - 1$, $c = c + 1$. Repeat step* (C) *until $r \leqslant c + 1$.*

(D) *Increment $WN = WN + 1$ and reset $CT = d$. Go back to step* (B) *unless $2(WN) + 1 > d$ in which case we are done.*

Proof. As before put $H = (h(r, c))$. Let a be a positive integer less than $l/4$. Suppose $[al/c] + 1 = R > T = [al/(c+1)] + 1$ with $d > c > a$. We assert that then $h(c+1, s) = 1$ for $s = T, \ldots, R-1$. Well $R - 1 \leqslant al/c < R$ so $sa/(R-1) \geqslant sc/l > sa/R$. Since $s \leqslant R - 1$ and $(sc, l) = 1$, we have $a > sc/l$. Similar considerations show $s(c+1)/l > a$ so $h(c+1, s) = [(c+1)s/l] - [sc/l] = a - (a-1) = 1$ and the assertion is proved.

Conversely, assume $h(c+1, s) = 1$ for some s. We assert that then $[al/(c+1)] + 1 \leqslant s \leqslant [al/c]$ where $a = [(c+1)s/l] < l/4$. Let $T = [al/(c+1)] + 1$ and $R = [al/c] + 1$. By our assumption, $cs/l < a < (c+1)s/l$ (there is no equality since l cannot divide a row or column index). The assertion follows easily.

We note that $WN \cdot l/c$ is never integral so $r = [WN \cdot l/c] + 1$ is merely the result of the division rounded upwards to the next integer. We give two examples. The nonzero integers in the matrices below stand for entries of H which are 1. The integers represent consecutive divisions in the scheme of Theorem 1.3. For $l = 23$, the first division determines 5 entries, the second division 3 entries, etc.:

$l = 23$:

$$\begin{matrix}
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 \\
0 & 0 & 3 & 0 & 0 & 0 & 0 & 4 & 4 \\
0 & 2 & 0 & 0 & 0 & 5 & 5 & 0 & 0 \\
0 & 0 & 0 & 0 & 6 & 0 & 0 & 7 & 7 \\
1 & 0 & 0 & 5 & 0 & 0 & 8 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 8 & 0 & 0 & 9 \\
0 & 0 & 4 & 0 & 7 & 0 & 0 & 10 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 9 & 0 & 11;
\end{matrix}$$

$l = 37$:

$$\begin{matrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 3 & 3 & 0 & 0 & 0 & 0 & 0 & 5 & 5 & 5 & 5 \\
0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 6 & 6 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 7 & 7 & 0 & 0 & 0 & 10 & 10 & 10 \\
0 & 0 & 3 & 0 & 0 & 0 & 0 & 8 & 0 & 0 & 0 & 11 & 11 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 9 & 0 & 0 & 0 & 12 & 0 & 0 & 0 & 15 & 15 \\
0 & 2 & 0 & 0 & 0 & 8 & 0 & 0 & 0 & 13 & 0 & 0 & 16 & 16 & 0 & 0 \\
0 & 0 & 0 & 0 & 7 & 0 & 0 & 0 & 14 & 0 & 0 & 17 & 0 & 0 & 19 & 19 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 13 & 0 & 0 & 18 & 0 & 0 & 20 & 0 & 0 \\
1 & 0 & 0 & 6 & 0 & 0 & 12 & 0 & 0 & 18 & 0 & 0 & 21 & 0 & 0 & 23 \\
0 & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 17 & 0 & 0 & 22 & 0 & 24 & 24 & 0 \\
0 & 0 & 5 & 0 & 0 & 0 & 0 & 16 & 0 & 0 & 21 & 0 & 25 & 0 & 0 & 26 \\
0 & 0 & 0 & 0 & 10 & 0 & 0 & 0 & 0 & 20 & 0 & 24 & 0 & 0 & 27 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 15 & 0 & 19 & 0 & 0 & 0 & 0 & 27 & 0 & 28 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 23 & 0 & 26 & 0 & 28 & 0.
\end{matrix}$$

With the nonzero entries above replaced by 1's, the reader may easily verify that $H(23) = 3$ and $H(37) = 37$.

2. Analytic Results

In this section we derive upper and lower bounds on the value of $H(l)$. From the residues of the Dedekind zeta functions of $\mathbf{Q}(\exp 2\pi i/l)$ and $\mathbf{Q}(\cos 2\pi/l)$ at the point $s = 1$, it is easy to see that

$$H(l) = G(l) \prod_{\substack{\chi \text{ odd} \\ f_\chi = l}} L(1, \chi)$$

where $G(l) = 2l(l/4\pi^2)^{(l-1)/4}$ and the $L(s, \chi)$ are Dirichlet's L-functions. Kummer [7] asserted that $H(l)$ is asymptotic to $G(l)$ but this has never been proved. Since values of $H(l)$ for $l \leqslant 257$ have been checked by at least three independent sources [10, 18], we assume throughout the rest of this section that $l \geqslant 263$.

In order to approximate $H(l)$, it suffices to approximate $g(1)$ where $g(s) = \sum_{\chi \text{ odd } f_\chi = l} \ln L(s, \chi)$. If the complex variable $s = \sigma + it$, we may consider $g(s)$ as a regular single-valued function in the region $\sigma \geqslant u(t)$, $u(t) = 1 - \frac{1}{20} \ln(l(1 + |t|))$, for all $l \geqslant 211$ [11] unless $l \equiv 3 \bmod 4$. When $l \equiv 3 \bmod 4$, the quadratic character $\chi^* \bmod l$ is odd and it is possible that there is a "Siegel zero" of $L(s, \chi^*)$ on the real axis between $\frac{1}{2}$ and 1. We can bound b, the exceptional zero, away from 1 by using the mean value theorem. Let $u = u(0) = 1 - \frac{1}{20} \ln l$, and let h be the class number of $\mathbf{Q}((-l)^{1/2})$. We have $\pi h/l^{1/2} = L(1, \chi^*) = (1 - b)\, L'(c, \chi^*)$ with $u < c < 1$ if $b \geqslant u$. Standard techniques show that

$$|L'(c, \chi^*)| \leqslant \sum_{a=1}^{d} \left| \frac{\ln a}{a^u} - \frac{\ln(l-a)}{(l-a)^u} \right| + \frac{\ln l}{l^u}\, T$$

where T is a uniform bound on the trigonometric sums $\sum_{a=1}^{n} \chi^*(a)$. The Polya–Vinogradov inequality [1, p. 173] allows us to take $T = l^{1/2} \ln l$. Then

$$\begin{aligned} |L'(c, \chi^*)| &\leqslant e^{0.05} \sum_{a=2}^{d} \ln a/a + e^{0.05} \ln^2 l/l^{1/2} \\ &< 0.53(\ln^2 l - 2 \ln l \ln 2 + \ln^2 2 + \ln^2 l/2l^{1/2}) \\ &< 0.53 \ln^2 l. \end{aligned}$$

Hence, $b \geqslant u$ implies $b \leqslant 1 - \pi h/0.53 l^{1/2} \ln^2 l$. Consequently, when $118h \geqslant l^{1/2} \ln l$ there is no exceptional zero in the region $\sigma \geqslant u(t)$. Since

$h \geqslant 3$ for $l \geqslant 263$, we see that this is certainly true for $l < 2137$. In this paper we are mainly concerned with bounds on $H(l)$ for small values of l, $l < 1000$, say, so we assume that $g(s)$ is single valued in $\sigma \geqslant u(t)$ for the primes l under our consideration. In a subsequent paper we will show that the methods of this section can be used to improve Lepistö's bounds [12] on $\ln(H(l)/G(l))$ for large l. The results of this section are an improvement on Lepistö's bounds for small l.

We will ultimately use the mean-value theorem to approximate $g(1)$ so we study $g(s)$ and its derivative on the real axis to the right of 1.

We can write $g(s)$ as a Dirichlet series for $\sigma > 1$

$$g(s) = d\left\{ \sum_{\substack{p,j \\ p^j \equiv 1(l)}} \frac{1}{jp^{js}} - \sum_{\substack{p,k \\ p^k \equiv -1(l)}} \frac{1}{kp^{ks}} \right\}$$

where p's are primes and j and k are natural numbers. Since the reduced residues modulo l form a cyclic group, the prime p will have some power congruent to -1 mod l if and only if p has even order modulo l. Hence, the Dirichlet series becomes

$$g(s) = d\left\{ \sum_{\substack{f \mid d \\ f \text{ odd}}} f^{-1} \sum_{\substack{p \text{ of} \\ \text{order } f \\ \text{mod } l}} - \ln(1 - p^{-fs}) - \sum_{f \mid d} f^{-1} \sum_{\substack{p \text{ of} \\ \text{order } 2f \\ \text{mod } l}} \ln(1 + p^{-fs}) \right\}$$

$$= d\left\{ \sum_{\text{odd } f \mid d} A(f, s) - \sum_{f \mid d} B(f, s) \right\}, \qquad \text{say.} \tag{2.a}$$

We will need some auxiliary lemmas in order to bound the A's and the B's.

LEMMA 2.1. *Let $I(a, b)$ denote $\int_a^b w^{-1}e^{-w}\,dw$. Then for $0 < a < 1$ we have $I(a, 1) < a - \ln a - 0.75$ and $I(a, \infty) < a - \ln a - 0.53$.*

Proof. For the first inequality notice that $I(a, 1) < \int_a^1 (x^{-1} - 1 + x/2)\,dx$. For the second inequality it suffices to show that $I(1, \infty) < 0.22$. Using the first few terms of its Taylor series as an upper bound for $w^{-1}e^{-w}$, we see that $I(1, 4) < 0.2157$ and from elementary estimates we see that $I(4, \infty) < e^{-4}/4 - e^{-5}/20 - e^{-6}/30 - \cdots < 0.0042$.

The above integral is useful because of the following

LEMMA 2.2. *Let f be a positive integer, $\epsilon = \pm 1$, and σ, β real numbers greater than 1. Put $r(\sigma, x) = (\epsilon/f)\ln(1 + \epsilon x^{-f\sigma})$. Let M be any modulus greater than 1. Put $K = M\beta - \epsilon$, $\beta^* = \beta - M^{-1}$ if $\epsilon = +1$, and $\beta^* = \beta$ if $\epsilon = -1$. Then if $K > M$ we have*

$$\sum_{\substack{p \geqslant K \\ p \equiv a(M)}} r(\sigma, p) < 2\sigma I((f\sigma - 1)\ln \beta^*, \infty)/\varphi(M)\, M^{f-1}(M^{\sigma-1})^f.$$

Proof. Let

$$P(x) = P(x, M, a, \beta) = \sum_{\substack{p \leqslant x \\ p \geqslant K \\ p \equiv a(M)}} 1 = \sum{}' 1.$$

Then $\sum' r(\sigma, p) = \sum_{n=m}^{\infty} (P(n) - P(n-1))\, r(\sigma, n)$ where $m = K$ or $[K] + 1$ according as K is an integer or not. Hence,

$$\sum{}' r(\sigma, p) = \sum_{n=m}^{\infty} \int_n^{n+1} \left(-\frac{\partial}{\partial x} r(\sigma, x) \right) P(n)\, dx$$

by partial summation. Using the large sieve inequality $P(x) < 2x/\varphi(M)\ln(x/M)$ which is valid for $x > M$ (see [14; 4, p. 124]) we obtain

$$\sum{}' r(\sigma, p) < \frac{2\sigma}{\varphi(M)} \int_K^{\infty} \frac{dx}{(x^{f\sigma} + \epsilon) \ln(x/M)}.$$

For $\epsilon = -1$ we see that $(x^{f\sigma} - 1) \ln(x/M) > (x-1)^{f\sigma} \ln((x-1)/M)$ so

$$\begin{aligned} \sum{}' r(\sigma, p) &< \frac{2\sigma}{\varphi(M)} \int_{M\beta}^{\infty} \frac{dx}{x^{f\sigma} \ln(x/M)} \\ &= \frac{2\sigma}{\varphi(M)} \frac{M^{1-f}}{(M^{\sigma-1})^f} \int_{\beta}^{\infty} \frac{dy}{y^{f\sigma} \ln y}. \end{aligned}$$

The result follows upon making the substitution $w = (f\sigma - 1) \ln y$. Similar reasoning applies when $\epsilon = 1$ since then $M\beta^* = K$ and $(x^{f\sigma} + 1)^{-1} < x^{-f\sigma}$.

COROLLARY 2.3. *When $\sigma > 1$, we have*

$$\begin{aligned} dA(1, \sigma) &< \sigma l^{1-\sigma}\{(\sigma - 1) \ln 2 - \ln(\sigma - 1) - 0.16\}, \\ dB(1, \sigma) &< \sigma l^{1-\sigma}\{(\sigma - 1) \ln 2 - \ln(\sigma - 1) - 0.16\}, \\ dA(1, \sigma) + dB(1, \sigma) &< \sigma l^{1-\sigma}\{3(\sigma - 1) \ln 2 - 2 \ln(\sigma - 1) - 1.02\}. \end{aligned}$$

Proof. Use Lemmas 2.1 and 2.2 with $\beta = 2$ or 4 noting that $2l - 1$ and $2l + 1$ are not both primes.

COROLLARY 2.4. *Let the positive integer a represent a reduced residue class* mod l *of order v greater than 2. Let $\epsilon = -1$, $f = v$ if v is odd and $\epsilon = 1$, $f = v/2$ if v is even. Put $r(\sigma, x) = (\epsilon/f) \ln(1 + \epsilon x^{-f\sigma})$ for $\sigma \geqslant 1$. Then*

$$\sum_{\substack{p \equiv a(l) \\ p > l}} r(\sigma, p) < d^{-1} \frac{\sigma}{(l^{\sigma-1})^f} \frac{(f-1) \ln l - (f/2)}{f l^{f-1}}$$

Proof. Notice that $a \geqslant (l-\epsilon)^{1/f}$. Hence the summation on the left-hand side is over primes greater than $\beta l - \epsilon \geqslant l + (l-\epsilon)^{1/f}$. Now apply Lemma 3.2.

We see that we can now estimate most of $g(s) = d\{\sum A - \sum B\}$ for $s = \sigma > 1$. It remains to consider the contribution of primes less than l. For a particular p, we have $-\ln(1-p^{-f\sigma}) < (p^f-1)^{-\sigma}$ and $\ln(1+p^{-f\sigma}) < p^{-f\sigma}$ so the contribution of p to $g(\sigma)$ may be estimated by either $(kl)^{-\sigma}$ or $(k(l-1))^{-\sigma}$ where $p^f + \epsilon = kl$. It is useful to know the following

LEMMA 2.5. *Let M be an odd prime power and let $f \geqslant 2$ be an integer dividing $\varphi(M)$. Then there is at most one prime p of order f modulo M with $p^f < M^2$. Also there is at most one odd prime p of order $2f$ with $p^f \equiv -1 \bmod M$ and $p^f < M^2$.*

Proof. Let z represent an element of order $2F$ modulo M with $z^{2F} < M^2$. Then $z^F < M$ and $z^F \equiv -1 \bmod M$ since the reduced residues modulo M form a cyclic group with a unique element of order two. Hence $z^F = M-1$ so z is even.

Suppose $g_1 < g_2$ are the least positive representatives in $\mathbf{Z}$ of elements of order $2F+1 = f$ modulo M with $g_i^f < M^2$. When $f = 3$, g_1 and g_2 are related by $g_2 = M - g_1 - 1$. Then $M/2 < g_2 < M^{2/3}$ implies $M = 7$ and so $g_2 = g_1^2 = 4$. When $f > 3$, consider the elements $1, g_1, g_1^2, \ldots, g_1^F, g_2, g_2^2, \ldots, g_2^F$. All these positive numbers are less than M by assumption so if two are congruent they are equal. If there is no duplication, these numbers must represent all f solutions of $x^f \equiv 1 \bmod M$. Now $g_1 g_2 < M^{4/f} < M$ and $g_1 < g_2 < g_1 g_2 < g_2^2$ so $g_1 g_2 = g_1^{A+1}$ and $g_2 = g_1^A$. If there is duplication, it is easy to see that it can be only of the form $g_2^B = g_1^A$. In either case we see that g_1 and g_2 have the same prime factors and the results follows.

Now suppose $g_1 < g_2$ are the least positive representatives of elements of order $2f$ with $g_i^f \equiv -1 \bmod M$ and $g_i^f < M^2$. When $f = 2F$ we see that $g_1^F, g_2^F, M - g_1^F, M - g_2^F$ all represent elements of order 4. Since there are only $\varphi(4) = 2$ elements of order 4 modulo M, $g_i^F \equiv M - g_j^F \bmod M$ with $i \neq j$ and thus $M = g_i^F + g_j^F$. Both of g_1 and g_2 cannot be odd primes because M is odd. When $f = 3$, $g_2 = M - g_1 + 1$ so $(M+1)/2 \leqslant g_2 < M^{2/3}$, a contradiction since $2f = 6$ must divide $\varphi(M)$. When $f = 2F+1 > 3$ consider

$$g_1, g_1^2, \ldots, g_1^F, g_2, g_2^2, \ldots, g_2^F, M - g_1, \ldots, M - g_1^F, M - g_2, \ldots, M - g_2^F.$$

If these are all distinct, they represent all the elements in the cyclic group of order $2f$ except ± 1. So $g_1 g_2 \equiv \pm g_i^{A+1}$ and since $g_2 < g_1 g_2 < g_2^2 \leqslant g_2^F < M$ we see that either $g_j = g_i^A$ or $g_j + g_i^A = M$ with $i \neq j$. We get similar equations when there is duplication among the $4F$ numbers under consideration. The result follows as above since M is odd.

We are now ready to estimate the contributions of $A(f, \sigma)$ and $B(f, \sigma)$ to $g(\sigma)$ where $f > 1$.

LEMMA 2.6. *When* $\sigma > 1$ *we have*

(i) $\sum_{\substack{\text{odd } f \mid d \\ f>1}} A(f, \sigma) < 0.19 d^{-1} l^{1-\sigma}$,

(ii) $\sum_{\substack{f \mid d \\ f>1}} B(f, \sigma) < 0.28 d^{-1} l^{1-\sigma}$,

(iii) $\sum A(f, \sigma) + \sum B(f, \sigma) < 0.4 d^{-1} l^{1-\sigma}$.

Proof. Lemma 2.5 tells us that for (i) and (ii) there is at most one number in the sequence $2l + \epsilon$, $4l + \epsilon$,..., $l(l-1) + \epsilon$ corresponding to each value of f in the summation.

For (i) we note that $-\ln(1 - p^{-f\sigma}) < (p^{f\sigma} - 1)^{-1} < (p^f - 1)^{-\sigma}$. If $p^f < l^2$ and p is odd, then $p^f - 1 = 2l \cdot k$ where $1 \leqslant k \leqslant d$. For the prime 2 we note that $f \geqslant 13$ if $l \geqslant 263$ and $2^f \equiv 1 \bmod l$ so the prime 2 contributes at most $l^{-\sigma}/13$. For the odd primes with $p^f < l^2$, we get an upper bound of $(2l)^{-\sigma}\{(3 \cdot 1)^{-1} + (5 \cdot 3)^{-1} + (7 \cdot 2)^{-1} + (9 \cdot 4)^{-1} + (11 \cdot 6)^{-1} + (13 \cdot 7)^{-1} + (15 \cdot 9)^{-1} + (17 \cdot 10)^{-1} + \cdots\} < (2l)^{-\sigma}(0.6)$. Here we have noted that 3 divides one of any three consecutive numbers of the progression $2l + 1$, $4l + 1$,..., $l^2 - l + 1$ and also that the order of 3 mod l is not less than 7. For the odd primes with $p^f > l^2$ and $p < l$, we may use the upper bound $l^{-2\sigma}(\frac{1}{2} + \frac{3}{5} + \frac{5}{7} + \cdots + (2t-1)/(2t+1))$ by noting that 1 and a p with $p^f < l^2$ already account for two of the residue classes of order f. There are at most $l/6$ odd primes less than l. Hence $1 + 3 + \cdots + 2t - 1 = t^2 < l/6$ so we get an upper bound of $(l/6)^{1/2} l^{-2\sigma}$. From Corollary 2.4 we can bound the contribution of the primes

$$p > l \quad \text{by} \quad d^{-1} \frac{\sigma}{(l^\sigma - 1)^3} \left\{ \frac{2 \ln l - 1.5}{3l^2} + \frac{4 \ln l}{5l^4} \frac{l}{2} \right\} < 0.013 (l^{1-\sigma})^2 / dl.$$

Putting these estimates together we see that for $\sigma > 1$,

$$\sum_{\substack{\text{odd } f \mid d \\ f>1}} A(f, \sigma) < d^{-1} l^{1-\sigma} \left(\frac{1}{26} + \frac{0.60}{4} + \frac{0.013}{l} \right) < 0.19 d^{-1} l^{1-\sigma}.$$

We proceed similarly for (ii). We have $\ln(1 + p^{-f\sigma}) < p^{-f\sigma} \leqslant (k(l-1))^{-\sigma}$ if $p^f = kl - 1$. For the prime 2, the numbers $2^{11} + 1 = 3 \cdot 683$, $2^{13} + 1 = 3 \cdot 2731$, and $2^{16} + 1 = 65{,}537$ are the smallest numbers of the form $2^f + 1$ which have prime factors larger than 262. We see that we can bound the contribution of the prime 2 to $\sum B(f, \sigma)$ by $(2d)^{-\sigma}/16$. For the prime 3,

$3^7 + 1 = 4 \cdot 547$, and, as before, 3 divides one of any three consecutive numbers in the sequence $2l - 1$, $4l - 1$,..., $l^2 - l - 1$. Hence, by Lemma 2.5 the odd primes with $p^f < l^2$, $f \geqslant 2$, $p^f \equiv -1 \bmod l$ have a contribution to the sum in (ii) bounded by $(4d)^{-\sigma}\{(2 \cdot 1)^{-1} + (3 \cdot 3)^{-1} + (4 \cdot 4)^{-1} + (5 \cdot 6)^{-1} + (6 \cdot 7)^{-1} + (7 \cdot 2)^{-1} + (8 \cdot 9)^{-1} + (9 \cdot 10)^{-1} + (10 \cdot 12)^{-1} + (11 \cdot 13)^{-1} + (12 \cdot 15)^{-1} + \cdots\} < 0.92(4d)^{-\sigma}$. For primes $p > l$, Corollary 2.4 shows that they contribute no more than ·

$$(d^{-1}\sigma/l^{(\sigma-1)2})\left(\frac{\ln l - 1}{2l} + \frac{2 \ln l}{3l^2} + \frac{3 \ln l}{4l^3}\, l\right) < 0.5(\ln l)^{1-\sigma}/dl.$$

Putting our estimates together, we see that

$$\sum_{\substack{f \mid d \\ f>1}} B(f, \sigma) < d^{-1}l^{1-\sigma}\left(\frac{1}{32} + \frac{0.92}{4} + \frac{0.5 \ln l}{l}\right) < 0.28l^{1-\sigma}/d.$$

Lastly, for (iii) we notice that 3 divides one of $2kl \pm 1$ whenever lk is prime to 3. Proceeding as above we would sum the reciprocals of $2 \cdot 1$, $3 \cdot 2$, $3 \cdot 3$, $4 \cdot 3$, $5 \cdot 4$, $5 \cdot 5$, $6 \cdot 6$, $7 \cdot 1$, $7 \cdot 6$, $8 \cdot 7$, $9 \cdot 8$, $9 \cdot 9$, $10 \cdot 9$, $11 \cdot 10$, $11 \cdot 11$, $12 \cdot 12$, $13 \cdot 12$, $13 \cdot 13$,... and obtain the result that the sum in (iii)

$$\sum A(f, \sigma) + \sum B(f, \sigma) < d^{-1}l^{1-\sigma}\left(\frac{1}{26} + \frac{1.40}{4} + \frac{0.013 + 0.5 \ln l}{l}\right) < 0.4d^{-1}l^{1-\sigma}.$$

We can now obtain both upper and lower bounds on $g(\sigma)$ for $\sigma > 1$ from (2.a). Moreover, by examining the proofs of Lemmas 2.2 and 2.6 we can see that for $v > 0$ we have proved that

$$|g(1 + v + it)| \leqslant \frac{1 + v}{l^v}\left\{3v \ln 2 - 2 \ln v - 1.02 + \frac{0.4}{1 + v}\right\}. \quad (2.b)$$

Denote the expression on the right-hand side by $B(v)$.

Now let $E(s) = \prod L(s, \chi)$ where the product is over all d odd Dirichlet characters of conductor l. Then $E(s)$ is an entire function and $E(s) = \exp(g(s))$ when $g(s)$ is defined. In particular, for $v > 0$ we have by (2.b) $|E(1 + v + it)| \leqslant \exp(B(v))$.

The functional equation for Dirichlet's L-functions with primitive characters shows us that

$$\left(\frac{\pi}{l}\right)^{-sd/2}\left(\Gamma\left(\frac{1 + s}{2}\right)\right)^d E(s) = W\left(\frac{\pi}{l}\right)^{-d(1-s)/2}\left(\Gamma\left(\frac{1 + 1 - s}{2}\right)\right)^d E(1 - s)$$

where W is a constant of absolute value one. We have, therefore,

$$|E(s)| \leqslant \left(\frac{\pi}{l}\right)^{d(\sigma-0.5)} \left|\Gamma\left(\frac{1}{2}+\frac{1-s}{2}\right)/\Gamma\left(\frac{1}{2}+\frac{s}{2}\right)\right|^{d} |E(1-s)|. \quad (2.c)$$

Following an idea of Rademacher we can now prove

THEOREM 2.7. *For* $\frac{1}{2} \geqslant v > 0$, $\sigma = \operatorname{Re} s \in (-v, 1+v)$, *and for all primes* $l \geqslant 263$ *the inequality*

$$\left|\prod_{\substack{\chi \text{ odd} \\ f_\chi = l}} L(s,\chi)\right| \leqslant \left(\frac{l\,|\,1+s\,|}{2\pi}\right)^{((l-1)/2)((1+v-\sigma)/2)} \exp(B(v))$$

holds where $B(v) = l^{-v}(1+v)(3v \ln 2 - 2\ln v - 1.02 + 0.4(1+v)^{-1})$.

Proof. We will use the following results of Rademacher which are special cases of Lemma 2 and Theorem 2, respectively, of [17]:

$$\left|\Gamma\left(\frac{1}{2}+\frac{1-s}{2}\right)/\Gamma\left(\frac{1}{2}+\frac{s}{2}\right)\right| \leqslant \left(\frac{1}{2}\,|\,1+s\,|\right)^{(1/2)-\sigma} \quad \text{for} \quad -\frac{1}{2} \leqslant \sigma \leqslant \frac{1}{2} \quad (2.d)$$

and

> Let $E(s)$ be regular analytic in the strip $S(a,b) = \{s \in \mathbf{C} \mid a \leqslant \sigma \leqslant b\}$ and satisfy for certain constants c, C $|E(s)| < C\exp(|t|^c)$. Suppose, moreover, that $|E(a+it)| \leqslant A\,|\,1 + a + it\,|^{\alpha}$ and $|E(b+it)| \leqslant B$ with $a > -1$ and $\alpha \geqslant 0$. Then in the strip $S(a,b)$ (2.e)
>
> $$|E(s)| \leqslant (A\,|\,1+s\,|^{\alpha})^{(b-\sigma)/(b-a)}\,(B)^{(\sigma-a)/(b-a)}.$$

Now $E(s)$ satisfies the growth condition of (2.e) because it is the product of functions which satisfy the same type of growth condition. Put $a = -v$ and $b = 1+v$. From (2.c) and (2.d) we see that for $\frac{1}{2} \geqslant v > 0$ we have

$$|E(-v+it)| \leqslant \left(\frac{2\pi}{l}\right)^{d(-v-(1/2))} |\,1-v+it\,|^{d((1/2)+v)} \exp(B(v)). \quad (2.f)$$

With $B = \exp(B(v))$, $\alpha = d(\frac{1}{2}+v)$, $A = (l/2\pi)^{\alpha}B$ the result follows from (2.e) by using (2.f) and $|E(1+v+it)| \leqslant B$.

COROLLARY 2.8. *For a prime* $l \geqslant 263$, $H(l)/G(l) = E(1) \leqslant e^{-2.75}(l-1)^2 \cdot \{\ln(l/\pi)\}^2$. *Alternatively,* $\ln(H(l)/G(l)) \leqslant 2\ln(l-1) + 2\ln\ln(l/\pi) - 2.75$.

Proof. Use Theorem 2.7 for $s = 1$ and $v = 8/((l-1)\ln(l/\pi))$.

The upper bound of Corollary 2.8 is sharper than the upper bound given in [13]. It is not so good as the upper bounds of Lepistö except for small primes congruent to 3 modulo 4. We can do better and also achieve lower bounds if we use the mean-value theorem to estimate $g(1)$. We need an estimate of $g'(s)$ for s near 1. For this we use the Borel–Carathèodory lemma:

LEMMA 2.9. *Let $R > 0$ and let $g(s)$ be regular in $|s - s_0| \leqslant R$. Suppose $\operatorname{Re} g(s) \leqslant M$ for $|s - s_0| = R$. Then in $|s - s_0| \leqslant \frac{1}{2}R$ we have $|g'(s)| \leqslant 8(M - \operatorname{Re} g(s_0))/R$.*

Proof. This is the special case $r = \frac{1}{2}R$ of Satz 4.2, p. 383 in [16].

The following estimate can be obtained for the derivative of $g(s)$.

PROPOSITION 2.10. *Let $r = 0.05/\ln l$, $s_0 = 1 + r$. Then for $|s - s_0| \leqslant r$ we have*

$$|g'(s)| \leqslant 4(l-1)\ln(l/3) + (\ln l)(236 + 218.4 \ln\ln l). \tag{2.g}$$

Proof. Let $v = 3/20 \ln l$. In the strip $S(-v, 1+v)$, Theorem 2.7 yields the bound $\operatorname{Re} g(s) \leqslant B(v) + d \cdot \frac{1}{2}(1 + v - \sigma) \cdot \ln(l\,|\,1 + s\,|/2\pi)$. We have $B(v) < 2.82 + 1.77 \ln\ln l$, and for $|s - s_0| \leqslant 2r$ we have $|1 + s|/2\pi < 3^{-1}$ and $1 + v - \sigma \leqslant 4r$. Thus $\operatorname{Re} g(s) \leqslant 2dr \ln(l/3) + 2.82 + 1.77 \ln\ln l$ for $|s - s_0| \leqslant 2r$. From (2.a), Corollary 2.3, and Lemma 2.6 we see that $-\operatorname{Re} g(s_0) \leqslant 0.96 \ln\ln l + 0.13$. Applying Lemma 2.9 now completes the proof.

The main result of this section is the following

THEOREM 2.11. *Let $l \geqslant 263$ be a prime for which all the Dirichlet L-functions with odd Dirichlet characters of conductor l are nonzero in the disk $|s - 1 - 0.05/\ln l| \leqslant 0.1/\ln l$. Then*

$$\ln(H(l)/G(l)) \leqslant \ln l + \ln\ln(l/3) + 2.79 + \frac{\ln l}{l \ln(l/3)}(54.6 \ln\ln l + 59)$$

and

$$-\ln(H(l)/G(l)) \leqslant \ln l + \ln\ln(l/3) + 2.88 + \frac{\ln l}{l \ln(l/3)}(54.6 \ln\ln l + 59).$$

In particular, $H(l) \leqslant (e^{3.52} l \ln(l/3))\, G(l)$.

Proof. Let $\sigma = 1 + 1/4(l-1)\ln(l/3)$ and apply the mean value theorem to $g(x)$ on the interval $[1, \sigma]$. Then $g(1) = g(\sigma) + (1 - \sigma) g'(c)$ with

$1 < c < \sigma$. As before, we may use (2.a), Corollary 2.3, and Lemma 2.6 to bound $g(\sigma)$ from above and from below. These bounds together with Proposition 2.10 provide the bounds on $g(1) = H(l)/G(l)$.

The results of Theorem 2.11 hold also for $l < 263$. Indeed, we have calculated $H(l)$ for $l < 521$ (see [10]) and the following was observed:

THEOREM 2.12. *For primes* l, $5 \leqslant l < 521$, $\prod_{\chi \text{ odd}\ f_\chi = l} L(1, \chi)$ *lies between* $\frac{2}{3}$ *and* $\frac{3}{2}$. *In particular,* $\frac{2}{3}G(l) < H(l) < \frac{3}{2}G(l)$ *for these primes.*

3. ARITHMETIC RESULTS

In this section we will use class field theory to prove some results about the prime factors of $H(l)$. Our number fields are all finite extensions of the field of rational numbers.

For a number field F, $C(F)$ will denote its ideal class group (in the wide sense) and the class number $h(F)$ of F is just the order of $C(F)$. Fix a prime p and let $S(F)$ denote the p-Sylow subgroup of $C(F)$. The Hilbert p-class field of F will be denoted $H(F)$. It is the maximal unramified Abelian extension of F with p-power degree and $\mathrm{Gal}(H(F)/F)$ is canonically isomorphic to $S(F)$ by the Artin reciprocity law. In particular $|H(F):F|$ is the exact power of p dividing $h(F)$. If F/K is normal and σ is an embedding of $H(F)$ which leaves K elementwise fixed, then $\sigma(H(F))/\sigma(F)$ is an unramified Abelian p-extension of $\sigma(F) = F$. By maximality $\sigma(H(F)) \subset H(F)$ so $H(F)/K$ is normal. The action of $\mathrm{Gal}(F/K)$ on $S(F)$ corresponds to group theoretic conjugation of $\mathrm{Gal}(H(F)/F)$ by $\mathrm{Gal}(H(F)/K)/\mathrm{Gal}(H(F)/F)$.

We assume all our fields to be either totally imaginary or totally real and with the property that there is a map (possibly the identity) J induced by complex conjugation on both the field and its ideal class group. We also assume that J commutes with all the automorphisms of our fields. Such fields are called J-fields. We will denote the maximal real subfield of F by F'. Under our assumption $|F:F'| = 1$ or 2. The relative class number $h^*(F)$ of F is the integer $h(F)/h(F')$. The relative class number of a totally real field is then 1 and the relative class number $h^*(F)$ of a totally imaginary field F is just the cardinality of $\mathrm{Ker}(C(F) \to^{1+J} C(F'))$ since this map is surjective.

If S is a finite Abelian group on which J acts, there are subgroups S^+, S^- of S which are just the kernels of $1 - J$ and $1 + J$, respectively. When S has odd order, $S = S^2$ and S^+, S^- are the images of $1 + J$ and $1 - J$, respectively. Furthermore, in that case $S = S^+ \times S^-$, an internal direct product.

By the p-rank of the finite Abelian group S, we mean the dimension of the $\mathbf{F}_p$-vector space $S \otimes_{\mathbf{Z}} \mathbf{F}_p \cong S/\{s^p \mid s \in S\}$.

The following lemmas are fundamental.

LEMMA 3.1. *Suppose F/K is normal with Galois group G and $S(F) = T \times V$, an internal direct product where G acts on T and on V. Then there is a subfield L of $H(F)$ normal over F with $\mathrm{Gal}(L/F) \cong T$, a G-isomorphism.*

Proof. As described above, $\mathrm{Gal}(H(F)/F)$ is G-isomorphic to $S(F)$ so we may view $S(F)$ as a subgroup of $W = \mathrm{Gal}(H(F)/K)$. Since $V^g \subset V$ for all g in G, $V \lhd W$. Let L be the subfield of $H(F)$ fixed by V. The result follows.

LEMMA 3.2. *Suppose F/K is normal with Galois group G whose order is prime to p. Suppose T is a subgroup of $S(F) \otimes_{\mathbf{Z}} \mathbf{F}_p$ on which G acts. Then there is a subfield L of $H(F)$ normal over F with $\mathrm{Gal}(L/F) \cong T$, a G-isomorphism.*

Proof. Let $S = S(F) \otimes_{\mathbf{Z}} \mathbf{F}_p$. Then S is G-isomorphic to $\mathrm{Gal}(N/F)$ where N is the fixed field of pth powers of elements of $S(F)$. Hence N is the maximal Abelian unramified extension of F of exponent p and as such is normal over K. Thus G acts on S, an $\mathbf{F}_p$-vector space. Since T is a subspace it has a complement V with $S = T \times V$. By averaging over G, we may assume that V is G-stable. Then proceed as in Lemma 3.1.

LEMMA 3.3. *Let p be an odd prime and let F be a totally imaginary J-field. Then $p \mid h^*(F)$ if and only if there exists an unramified Abelian extension L of F, $\mid L : F \mid = p^a > 1$, L/F' Galois, and $J\sigma J = \sigma^{-1}$ for all $\sigma \in \mathrm{Gal}(L/F)$.*

Proof. We remarked earlier that $h^*(F) = \mathrm{card}\, C(F)^-$. Hence $S(F)^-$ is nontrivial. Now apply Lemma 3.1 with $K = F'$, $S(F) = S^- \times S^+$.

Conversely, suppose F has a nontrivial unramified Abelian p-extension L with L/F' Galois and $J\sigma J = \sigma^{-1}$ for all $\sigma \in \mathrm{Gal}(L/F)$. Consider $M = FH(F')$. This is an unramified Abelian p-extension of F and $J\tau J = \tau$ for all $\tau \in \mathrm{Gal}(M/F)$. Since p is odd, L and M are linearly disjoint over F so the p-part of $\mid L : F \mid h(F')$ equals $\mid LM : F \mid$ which divides the p-part of $h(F)$.

We are now ready to prove our main results of this section.

THEOREM 3.4. *Let E/F be a cyclic extension of degree n with E/F' Galois. Let p be an odd prime not dividing n and suppose $S(\tilde{E})^- = 1$ for all $\tilde{E}$ with $F \subseteq \tilde{E} \subsetneq E$. Then the p-rank of $S(E)^-$ is divisible by $f =$ the order of p modulo n.*

Proof. We may assume that $S(E)^- \neq 1$ and hence that E is totally imaginary. Let $S = S(E) \otimes_{\mathbf{Z}} \mathbf{F}_p$. Then $S^- \neq 1$ and S^- has the same p-rank as $S(E)^-$. Let $G = \mathrm{Gal}(E/F)$. Since E is a J-field, we have $Jg = gJ$ for all g in G. Consequently, $S^- = S^{1-J}$ is invariant under G and hence also under $G' = \mathrm{Gal}(E/F')$. By Lemma 3.2 there is an extension L of E with L/F' Galois and $B = \mathrm{Gal}(L/E)$ G'-isomorphic to S^-.

Suppose $g \in G$ acts trivially on a subgroup $\tilde{B} \neq 1$ of B, $g \neq 1$. Since J inverts the elements of B, g has odd order and $\langle gJ \rangle$ contains $\langle g \rangle$ as a subgroup of index 2. Let $\tilde{E}$ be the proper subfield of E fixed by $\langle g \rangle$. Then

$\tilde{E}$ is totally imaginary and $\tilde{E}'$ is the field fixed by $\langle gJ \rangle$. By Lemma 3.2 there is an extension $\tilde{L}$ of E with $\mathrm{Gal}(\tilde{L}/E)$ $\langle gJ \rangle$-isomorphic to $\tilde{B}$ and $\tilde{L}$ normal over $\tilde{E}'$ and hence over $\tilde{E}$. Let $A = \mathrm{Gal}(\tilde{L}/\tilde{E})$. Now $A/\tilde{B} \simeq \langle g \rangle$ and $\langle g \rangle$ acts trivially on $\tilde{B}$. Since the order of $\langle g \rangle$ is prime to the order of $\tilde{B}$, the group extension $A/\tilde{B}$ splits and we have the direct product $A \simeq \tilde{B} \times D$ where $D \simeq \langle g \rangle$ and J acts trivially on D. Let K be the fixed field of D so that $\mathrm{Gal}(\tilde{L}/K) = D$ and $\mathrm{Gal}(K/\tilde{E}) \simeq A/D \simeq \tilde{B}$, a nontrivial p-group which J inverts. Let P be any prime divisor of $\tilde{L}$ with inertia group T for $\tilde{L}/\tilde{E}$. Since $\tilde{L}/E$ is unramified at all prime divisors, $T \cap \tilde{B} = 1$. The groups $\tilde{B}$ and D have relatively prime orders so it follows that $T \subset D$. This shows that $K/\tilde{E}$ is unramified at all prime divisors. Since D is a normal subgroup of $\mathrm{Gal}(\tilde{L}/\tilde{E}')$, Lemma 3.3 implies that $S(\tilde{E})^- \neq 1$ contrary to hypothesis. This contradiction shows that a generator of G and all its nonidentity powers act nontrivially on B and its proper subgroups.

Any G-module which is a vector space over $\mathbf{F}_p$ is G-isomorphic to a sum of irreducible submodules of the semisimple algebra $\mathbf{F}_p[G]$. By identifying G with the group of nth roots of unity, we see that $\mathbf{F}_p[G] \simeq \oplus_{d|n} R_d$ where $R_d \simeq \mathbf{Z}[\zeta_d]/p\mathbf{Z}[\zeta_d]$, ζ_d a primitive dth root of unity, and g^d acts trivially on all constituents of R_d for all $g \in G$. By what we have seen above, the G-module S^- has all its irreducible constituents taken from R_n. Now R_n is the direct sum of the residue class fields of the primes above p in $\mathbf{Q}(\zeta_n)$. These fields are certainly irreducible G-modules and each has dimension f, the residue class degree, over $\mathbf{F}_p$. As is well known, f is the order of p modulo n.

COROLLARY 3.5. *Let $E \subset \mathbf{Q}(\exp 2\pi i/l)$ and suppose the relative class number of every proper nonreal subfield of E is prime to p, an odd prime not dividing $|E : \mathbf{Q}|$. Then the p-rank of $C(E)^-$ is divisible by f, the order of p modulo $|E : \mathbf{Q}|$. In particular, $p \mid h^*(E)$ implies $p^f \mid h^*(E)$.*

We also have the following "pushing-down" property.

THEOREM 3.6. *Let E/F be a totally ramified p-extension, p an odd prime, where exactly one prime divisor of F ramifies in E. Then $p \mid h^*(E)$ if and only if $p \mid h^*(F)$.*

Proof. We may assume E, and hence F also, is totally imaginary. If $p \mid h^*(E)$, then by Lemma 3.3 there is an unramified Abelian extension L of E, $|L : E| = p^a > 1$, L/E' Galois, and $J\sigma J = \sigma^{-1}$ for all $\sigma \in \mathrm{Gal}(L/E) = S$. Assume L is the maximal field satisfying all these properties. Now J commutes with all the elements of $A = \mathrm{Gal}(E/F)$ since E is a J-field and so E/F' is Galois. By the maximality of L, L/F' and hence L/F are Galois. Let $B = \mathrm{Gal}(L/F)$ and let T be the inertia subgroup of B for any prime of L lying above P, the unique prime of F ramified in E. Since L/E is unramified and

E/F is totally ramified, T has $|E:F|$ elements and $S \cap T = 1$. Since B is a p-group, T is contained in N, a normal subgroup of B of index at least p. Let N be the smallest such normal subgroup of B. The inertia subgroups of all the primes of L lying above P are conjugate in B and are thus contained in N. Let K be the subfield of L fixed by N. Then K is the maximal subextension of L/F which is unramified and so is Galois over F'. Since $|B:N| > 1$, $|K:A| > 1$. Now B/N is a homomorphic image of S, so K/F is an Abelian extension and J acts on B/N. Also, S has only the identity element in common with any B-conjugate of T so it is easy to see that J inverts the elements of B/N. By Lemma 3.3 then $p \mid h^*(F)$.

Conversely, if $p \mid h^*(F)$ let L be the Abelian extension of F described in Lemma 3.3. Since E/F is totally ramified, LE/E is an Abelian extension of E which by Lemma 3.3 shows that $p \mid h^*(E)$.

For applications of the above results to factoring $H(l)$ we need the "standard factorization" of $H(l)$. For more details see [5, Sections 31, 33].

Let χ be any Dirichlet character mod l of exact order $2d$. Let $ef = 2d$ with f odd and define $c_e = 1, 2, l$, or $2l$ as follows. Put $c_e = 1$ unless the corresponding f is a maximum or a minimum. When f is the largest odd divisor of d, $2 \mid c_e$. When $f = 1$, $l \mid c_{2d}$. We have $c_e = 2l$ only when d is a power of 2 and $e = 2d$. The algebraic number $b_f = (-1/2l)\sum_{a=1}^{l} \chi^f(a)a$ lies in $\mathbf{Q}(\exp 2\pi i/e) = K$ and we put $H_e(l) = c_e N_{K/\mathbf{Q}}(b_f)$ where $ef = 2d$, f odd.

What we have done is grouped together all of the factors of (1.a) which are conjugates of one another and redistributed the constants $2l$ so that

$$H(l) = \prod_{\substack{ef=l-1 \\ f \text{ odd}}} H_e(l) \tag{3.a}$$

is an expression for $H(l)$ as the product of rational integers. If $E \subset \mathbf{Q}(\exp 2\pi i/l) = L$, E totally imaginary of degree n, then

$$h^*(E) = \prod_{\substack{ef=n \\ f \text{ odd}}} H_e(l). \tag{3.b}$$

We now have the following results for the field L.

THEOREM 3.7. *Let p be an odd prime and c a positive integer. Suppose $cp^a \mid (l-1)$ and let E and F be the subfields of L of degree cp^a and c, respectively. Then $p \mid h^*(E)$ if and only if $p \mid h^*(F)$.*

Proof. We may assume that E and F are totally imaginary. Then the unique prime above l in F is the only prime which ramifies in E and it is totally ramified. Now apply Theorem 3.6.

THEOREM 3.8. *Let p be an odd prime not dividing e and let E be the unique subfield of L of degree e. If $p \nmid h^*(F)$ for every proper nonreal subfield F of E, then $H_e(l)$ is either prime to p or divisible by p^f where f is the order of p modulo e.*

Proof. By Corollary 3.5, we have $h^*(E)$ is either prime to p or divisible by p^f. Using (3.b), however, and our hypothesis we see that the p-parts of $h^*(E)$ and $H_e(l)$ are the same.

The results of Theorems 3.7 and 3.8 were known to Lehmer. He is able to prove slightly more general results using only elementary methods [8, 9]. In particular, he shows that $p \mid H_{ep}(l)$ if and only if $p \mid H_e(l)$ for any odd prime p with $ep \mid (l-1)$. A study of the action of $\mathrm{Gal}(L/\mathbf{Q})$ on $S(L)^-$ would probably give this result. For primes p, $p \nmid le$, Lehmer shows that the exact power of p dividing $H_e(l)$ is a multiple of f, the order of p modulo e. This seems to be similar to our result 3.4, but Lehmer's result is only about factors of class numbers, not about structures of class groups. Theorem 3.4, on the other hand, allows us to conclude immediately that the ideal class group of $\mathbf{Q}(\exp 2\pi i/41)$ has exponent 11 once we know that its order is 121.

As we remarked earlier we used the results of this paper to calculate $H(l)$ for $l < 521$ and partially factor these numbers. The details of these computations appear in [10].

ACKNOWLEDGMENTS

Computing facilities were provided by the University of Illinois Computing Center. We thank A. O. L. Atkin, Ben Setzer, and James Slifker for their assistance, the Institute for Advanced Study for its hospitality, and the National Science Foundation for its support.

REFERENCES

1. T. APOSTOL, "Introduction to Analytic Number Theory," Springer–Verlag, New York, 1976.
2. Z. BOREVICH AND I. SHAFAREVICH, "Number Theory," Academic Press, New York, 1966.
3. L. CARLITZ AND F. OLSON, Maillet's determinant, *Proc. Amer. Math. Soc.* **6** (1955), 265–269.
4. H. HALBERSTAM AND H.-E. RICHERT, "Sieve Methods," Academic Press, London, 1974.
5. H. HASSE, "Über die Klassenzahl abelscher Zahlkorper," Akademie–Verlag, Berlin, 1952.
6. K. IWASAWA, "Lectures on p-adic L-Functions," Princeton Univ. Press, Princeton, N.J., 1972.
7. E. KUMMER, Sur la theorie des nombres complexes composes de racines de l'unité et de nombres entiers, *J. Math. Pures Appl.* **16** (1851), 473; "Collected Works," Vol. I, p. 459.
8. D. H. LEHMER, "Factorization of certain cyclotomic functions," *Ann. of Math.* **34** (1933), 461–479.

9. D. H. LEHMER, Prime factors of cyclotomic class numbers, *Math. Comp.*, to appear.
10. D. H. LEHMER AND J. MASLEY, Table of the cyclotomic class numbers $h^*(p)$ and their factors for $200 < p < 521$, *Math. Comp.*, to appear.
11. T. LEPISTÖ, A zero-free region for certain L-functions, *Ann. Acad. Sci. Fenn. Ser. A I*, **576** (1974), 1–13.
12. T. LEPISTÖ, On the growth of the first factor of the class number of the prime cyclotomic field, *Ann. Acad. Sci. Fenn. Ser. A I* **577** (1974), 1–21.
13. J. MASLEY AND H. MONTGOMERY, Unique factorization in cyclotomic fields, *J. Reine Angew. Math.* **286/287** (1976), 248–256.
14. H. MONTGOMERY AND R. VAUGHAN, On the large sieve, *Mathematika* (1973), 119–134.
15. M. NEWMAN, A table of the first factor for prime cyclotomic fields, *Math. Comp.* **24** (1970), 215–219.
16. K. PRACHAR, "Primzahlverteilung," Springer–Verlag, Berlin, 1957.
17. H. RADEMACHER, On the Phragmen–Lindelof theorem and some applications, *Math. Z.* **72** (1959), 192–204.
18. G. SCHRUTKA V. RECHTENSTAMM, Tabelle der (relativ-) Klassenzahlen von Kreiskorpern, *Abh. Deutsche Akad. Wiss. Berlin Math. Nat. Kl. Nr.* **2** (1964).